Smart Card Technology Capabilities

Won J. Jun

Giesecke & Devrient (G&D)

July 8, 2003

Table of Contents

- Smart Card Basics
- Current Technology
- Requirements and Standards
- Next Steps

Smart Card Basics

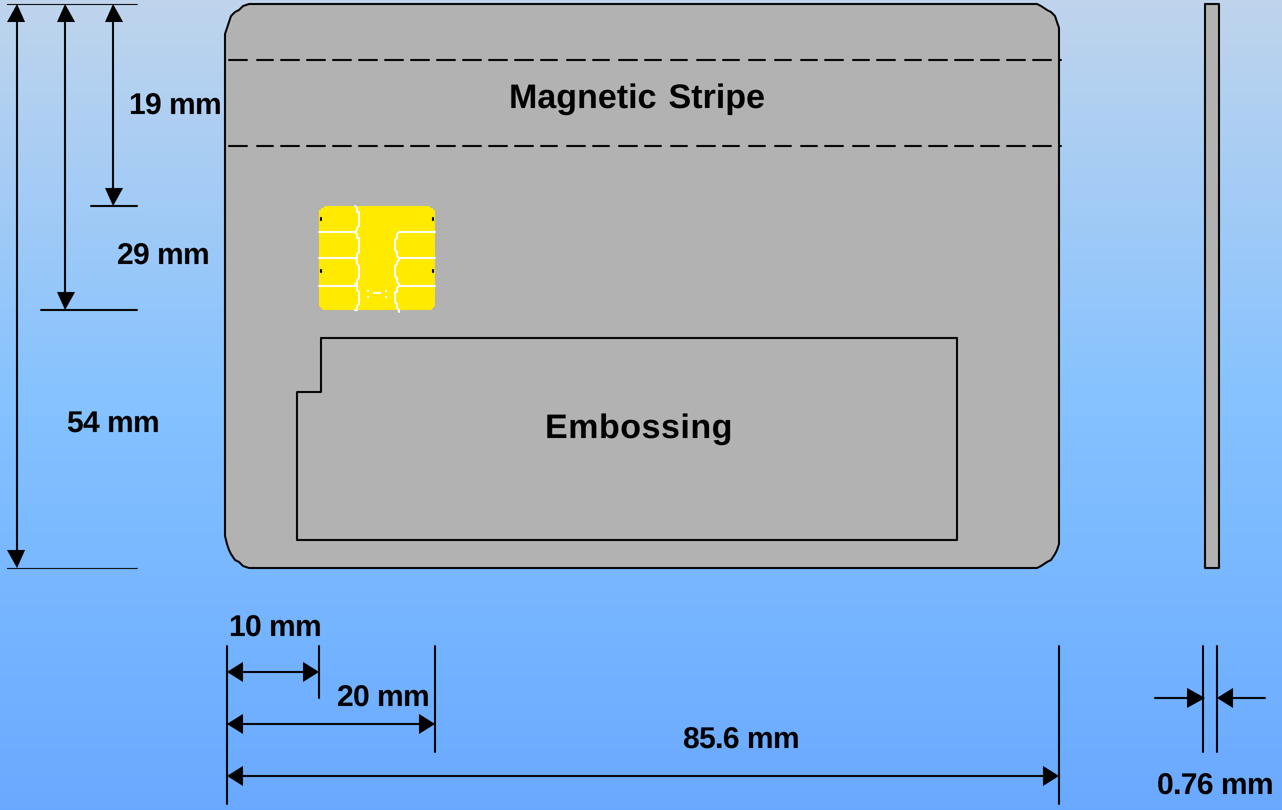
- Definition
- Components
- Different Types
- Standards and Specifications
- Applications

Definition

- What is a smart card?
  - A plastic card with an embedded microprocessor chip.
- What is the essence of a smart card?
  - Authentication
  - Data storage
  - Validation
  - Self-lock mechanism

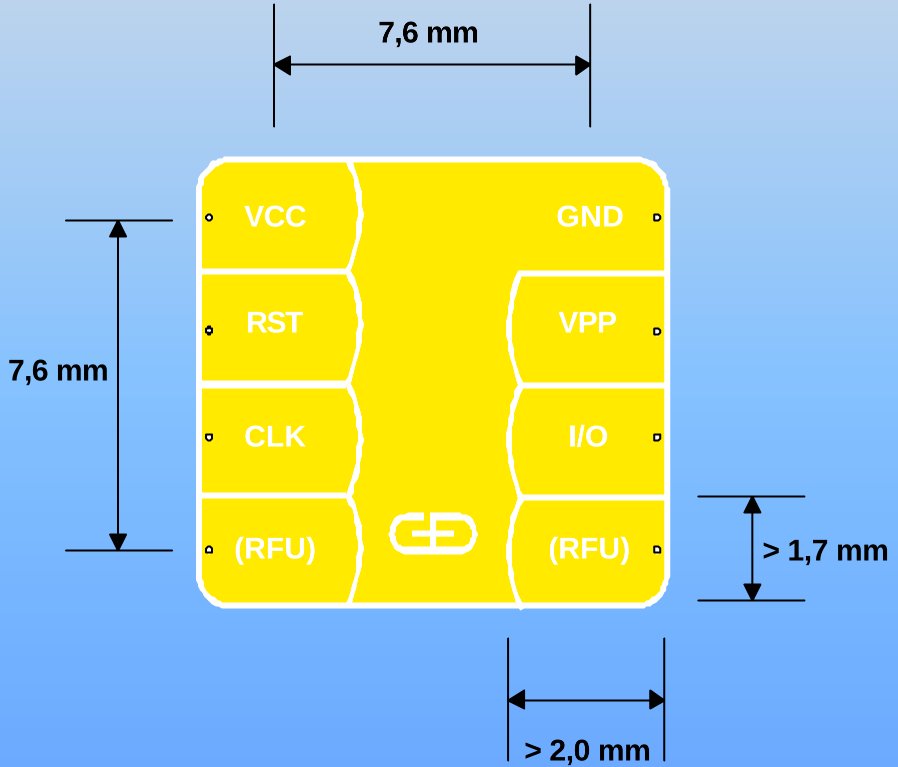
The Dimensions

Smart Card according to ISO/IEC 7810 and ISO/IEC 7816-2



The Contacts

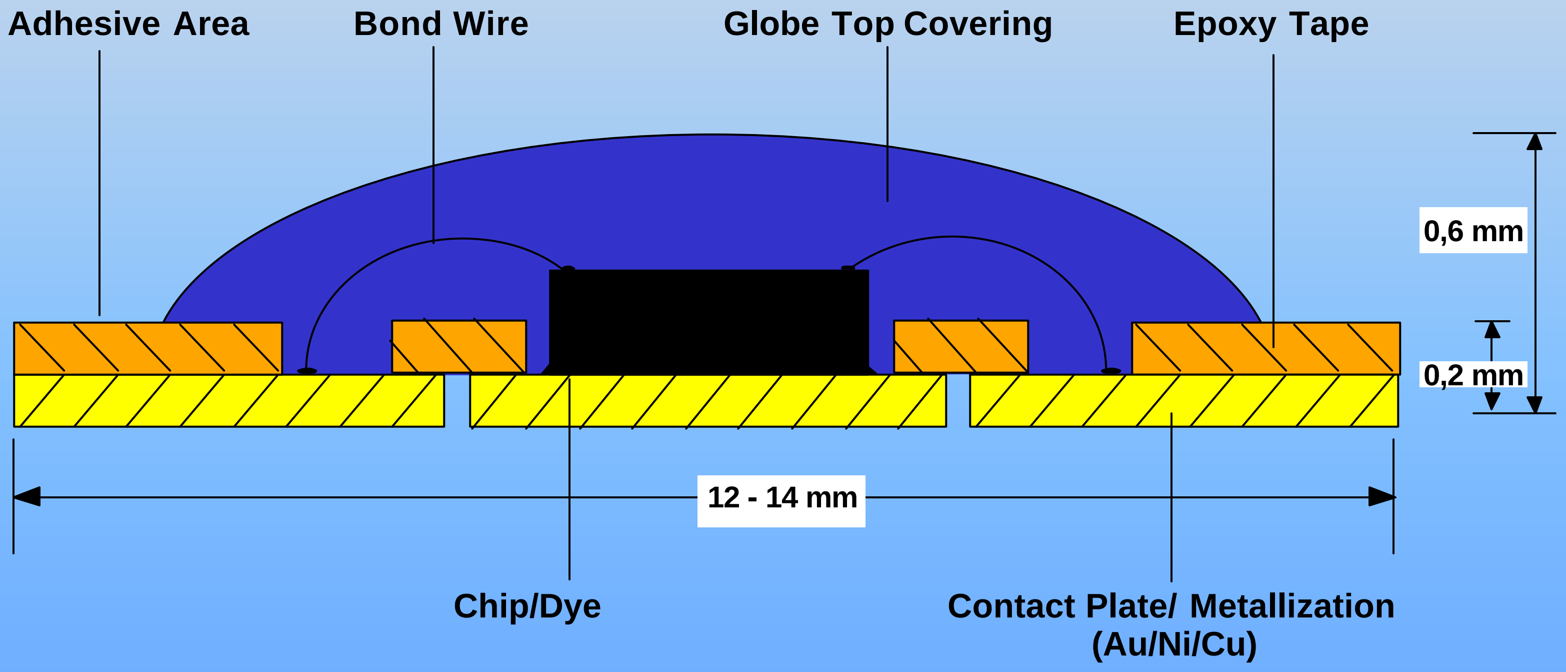
Contacts of the Smart Card Module according ISO/IEC 7816-2



VCC	Power Supply Voltage
RST	Reset
CLK	Clock
RFU	Reserved for Future Use
GND	Ground
VPP	Programming Voltage
I/O	Input/Output

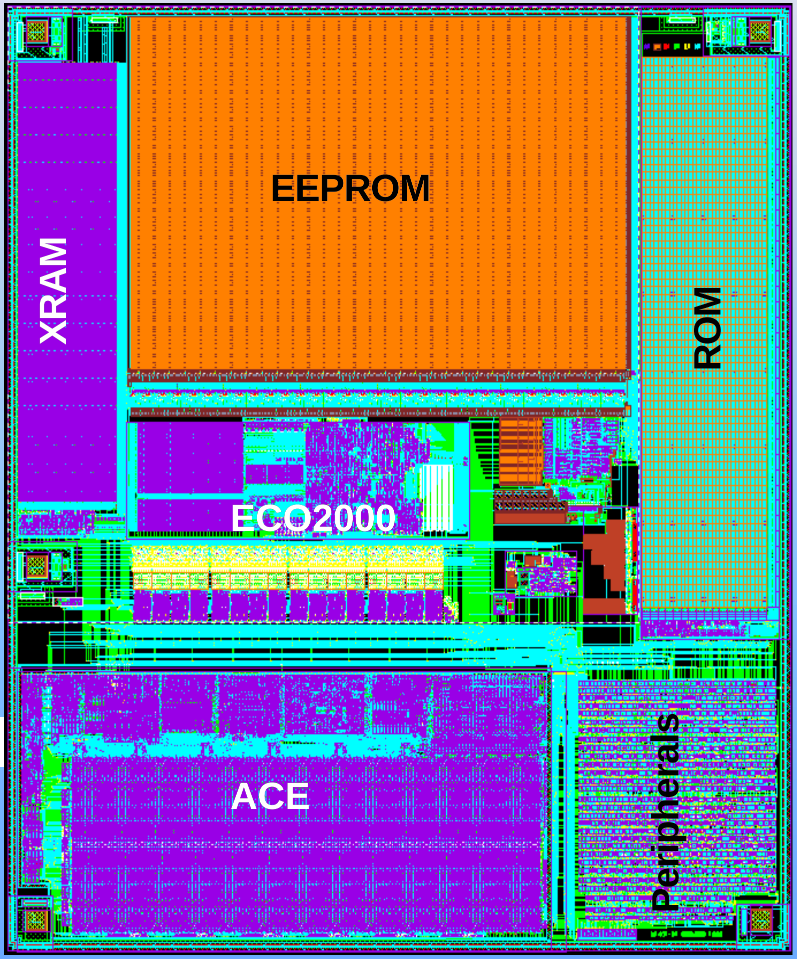
The Module

Cross-Section of a Smart Card Module

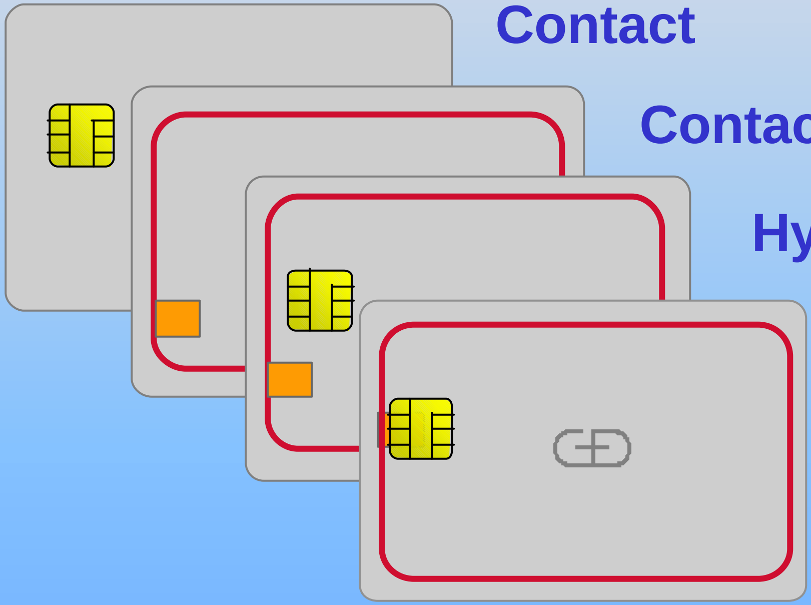


The Chip

- Features:
  - – 32 kByte ROM
  - – 16 kByte EEPROM
  - – 1.3 kByte RAM
  - – Crypto Unit ACE
- Chip size:
  - – Area = 21.23 mm²
  - – x = 4.28 mm, y = 4.96



Different Types



Contact

Contactless

Hybrid

Dual-Interface (Combi)

How Smart?

- Simple Memory Card
  - No Security
- Intelligent Memory Cards
  - Access Control Conditions for defined areas
  - Dedicated functionality (e.g., Telephone-Chip Card)
- Microprocessor Card
  - Microcomputer / Microcontroller
- Super Smart Card
  - Microcomputer, Keypad, Display, Battery, etc.

Relevant Standards and Specs

- ISO 7810
- ISO 7816
- ISO 14443 Types A and B
- Java Card 2.1.1 and 2.2
- Global Platform Card Specification 2.0.1’ and 2.1
- GSCIS v2.1 (draft)

Types of Usage

- Identification and authentication
- Encryption and digital signature (RSA 1024/2048 bit; on-card key-pair generation)
- Biometric (on-card matching)
- Secure Data storage
- Single Sign-on

Assessing the Current Technology

Areas to Assess:

- Card Operating System (COS)
- Protocol
- Memory capacity
- Functionality

Card Operating System

File-structure vs. Java Card

ISO 7816 part 4 +
compliant COS ↔ Java Card and
Global Platform
compliant COS

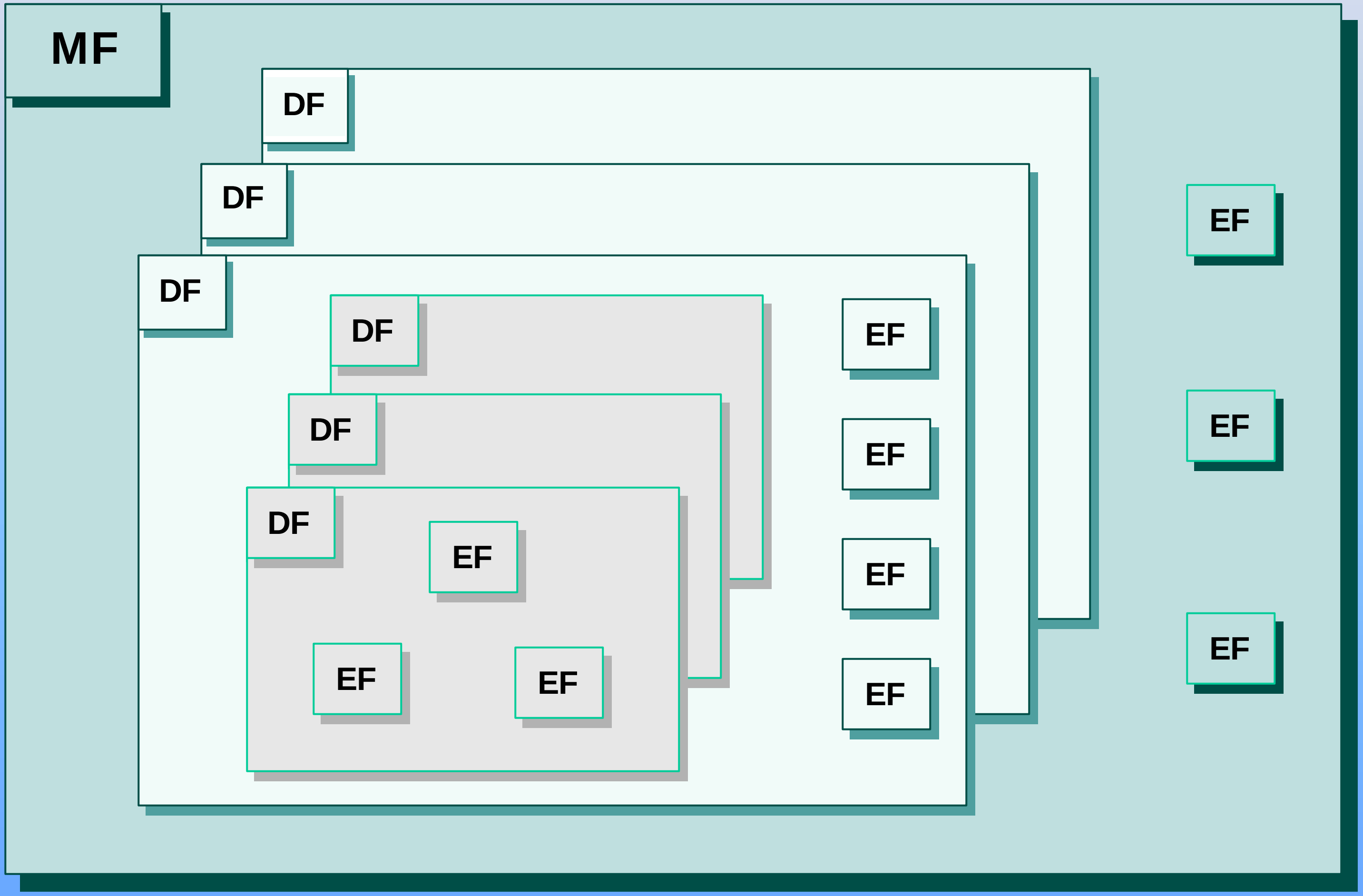
Analogous to

Unix ↔ Windows ®™

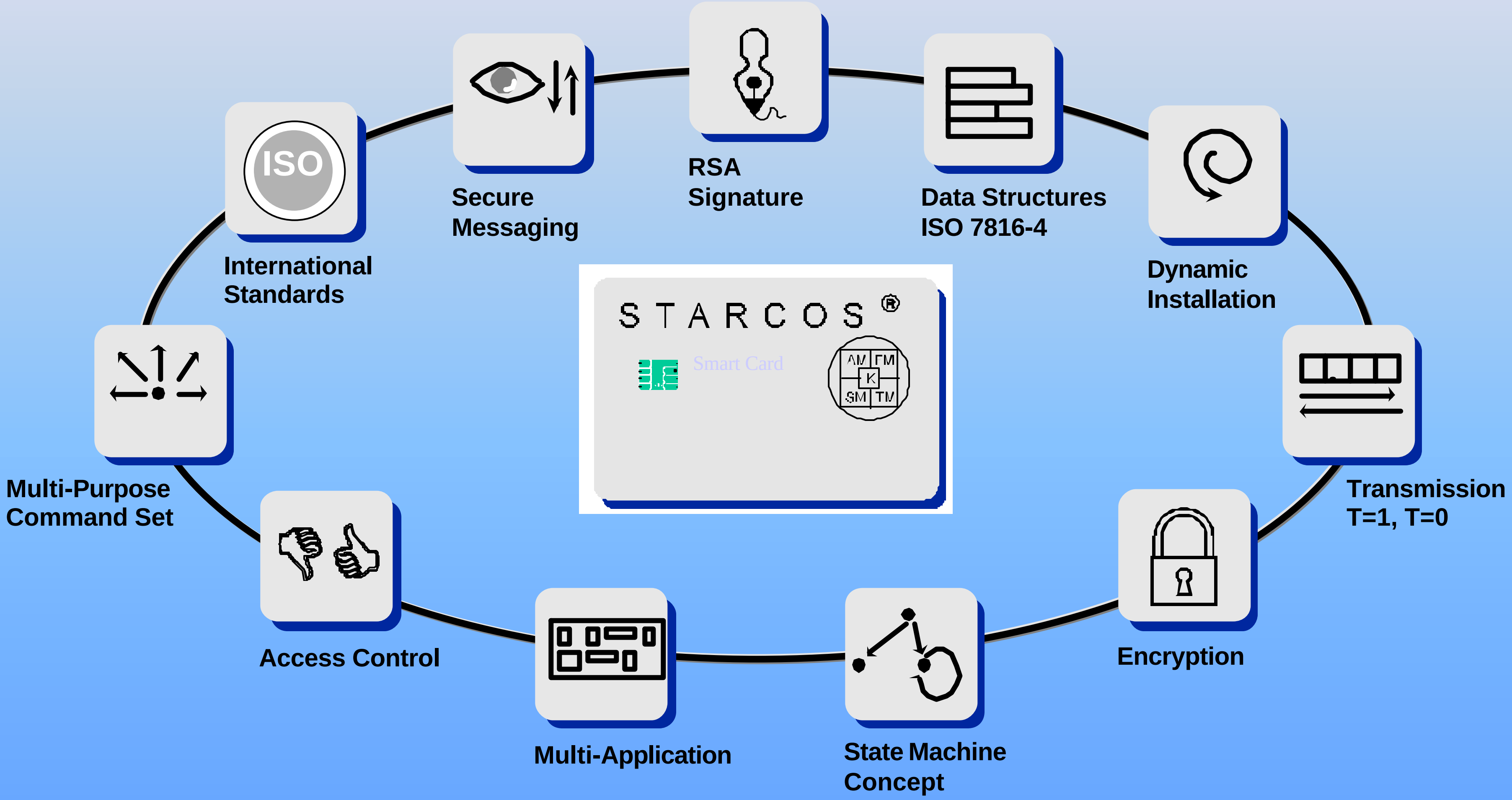
There are Pro's and Con's for both types of COS's. Both can be made secure and flexible. It is analogous to comparing Unix and Windows®™ operating systems. The philosophical arguments can be made for file-structure-based or Java-based card.

However……..Java Cards are in fashion!

File-Structure Based Smart Cards



Purpose of a Smart Card OS



International Standards

Secure Messaging

RSA Signature

Data Structures ISO 7816-4

Dynamic Installation

Transmission T=1, T=0

Encryption

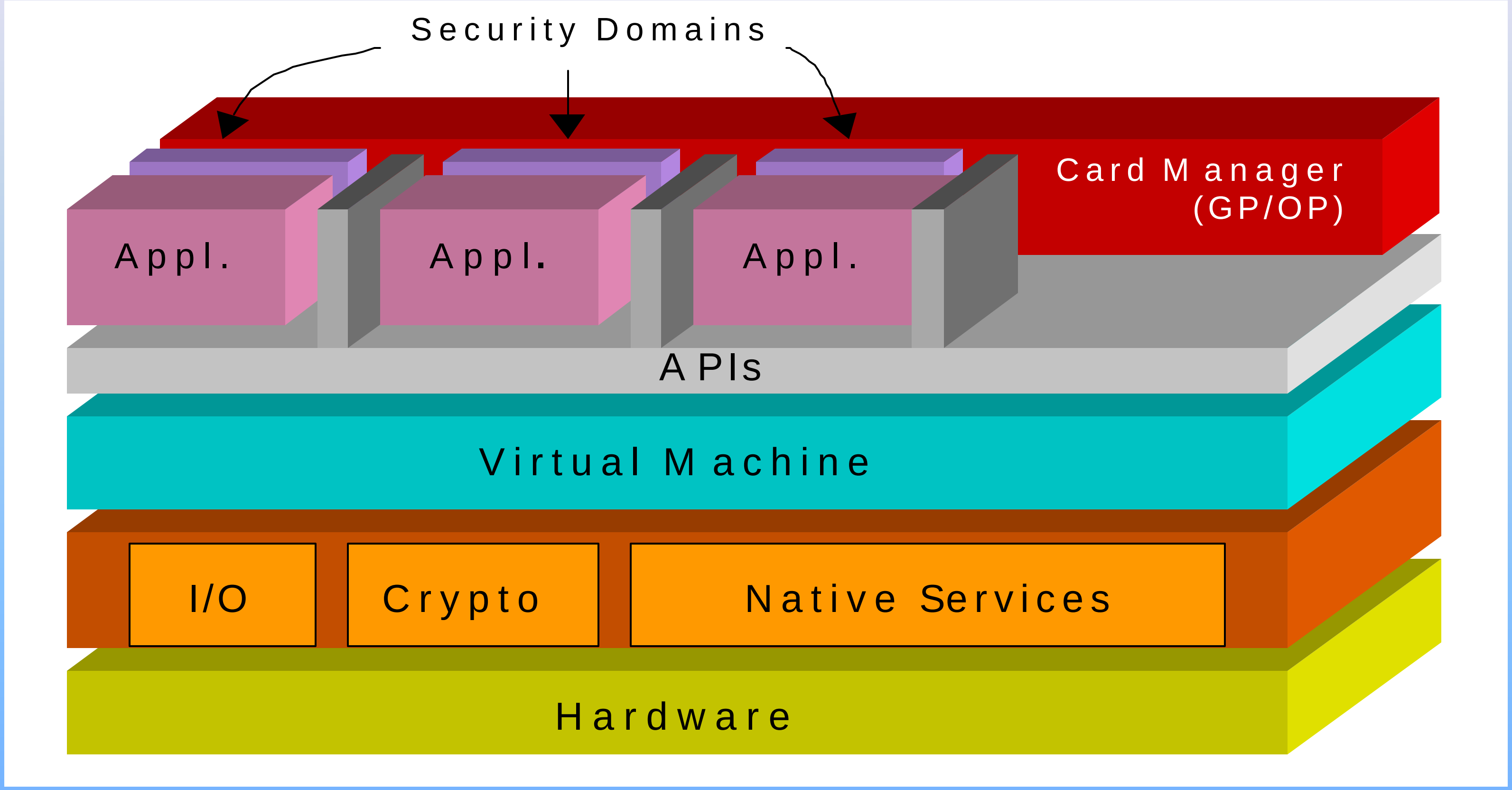
State Machine Concept

Multi-Application

Access Control

Multi-Purpose Command Set

Java Card Security



- Security is provided by the JCVM, Firewalls and Security Domains

Java Card Basics

- A multi-application smart card
  - Several applications can be loaded on to the same card
  - “Firewall” between applications
  - Sharing between applications
  - ISO-7816/4 compliant application selection.

- Smart card interoperable--
  - at the source code level
  - at the load file level
  - at the loader level.

Protocol

- T=0 : Byte transfer. Developed by the French
- T=1 : Block transfer. Developed by the Germans
- USB : Based on existing USB v.1.1+ Specs.

Memory Capacity

- 16 KB
- 32 KB *
- 64 KB
- 128 KB

* Currently most popular

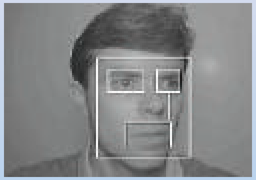
Functionality

Highlights:

- RSA 1024/2048 bit algorithms
- Triple-DES, SHA-1
- On-card key-pair generation
- On-card Biometrics matching engine

Biometrics On-card Matching

- **Main advantages:**

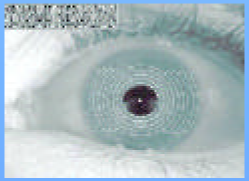


■ Sensor independent

- **Latest developments:**

■ Fingerprint on-card matching

■ Iris on-card matching

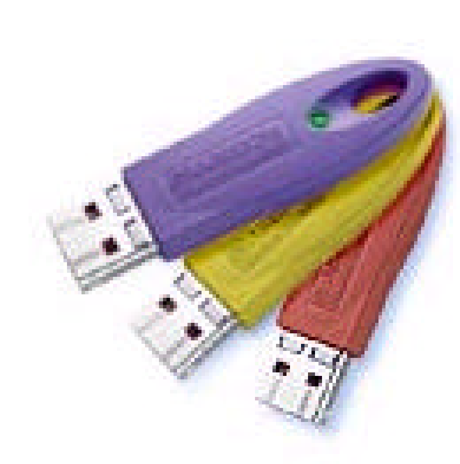


■ On-card matching Java applet

Basics of On-card Matching

- The actual data is preprocessed in the background system and sent to the card
- Biometric verification takes place on the chip card
- Reference data does not leave the card
- The card itself changes the security status (e.g., unblocks itself) after a successful verification.

Other Form Factors



- Smart chip with USB interface.
  - Same Chip Operating System as on smart card.
  - Connectivity through USB port. Smart card reader not necessary.

- Three features in one single USB device:
  - Multiapplication smart card operating system
  - Fingerprintsensor
  - Imageprocessing software

Current Trends

- Java Card 2.1
- Global Platform 2.0.1’
- 32 to 64K EEPROM
- On-card key-pair generation (RSA 1024-bit)
- Biometric on-card matching (fingerprint)
- Hybrid and composite card bodies (ISO 14443)
- FIPS 140-2, Level 2 or 3

Current Trends

Requirements and Standards

CAC Release 2.0 ICC Specification	
• Java Support	➢ Java Card 2.1
• Standards:	➢ ISO 7816, parts 1-7 ➢ T=0 ➢ EMV. ➢ Global Platform 2.0.1. ➢ DAP verification ➢ Delegated management and services ➢ ISO 10373 Parts 1-3 ➢ ISO 7810 ➢ GSCIS 2.0
• Micro-controller/ Processor:	➢ 32KB EEPROM ➢ 8-bit processor. ➢ Cypto co-processor

Requirements and Standards

CAC Release 2.0 ICC Specification (Cont’d)	
• Crypto Algorithms: • Digest Algorithms: • Key Exchange: • Signature Algorithms:	➢ Triple DES ➢ SHA-1 ➢ RSA ➢ RSA (1024-bit key length) ➢ FIPS PUB 180-1 Secure Hash Standard ➢ FIPS PUB 186-1 Digital Signature Standard
• On-Card Key Generation	➢ 30 seconds or less
• Security:	➢ FIPS 140, Level 2 or 3 validation ➢ Countermeasures for Differential Power Analysis and Simple Power Analysis Attacks

Requirements and Standards

Requirements on the horizon:

- ≥ 2048-bit key length
- On-card Biometric Verification
- Contactless PKI
- Hybrid and Dual-interface cards
- Super Smart Cards

Next Steps

- Standards are needed to address the coming requirements.
- Existing standards may need to be updated to accommodate the changing technology.
- Validations are needed to test conformance.